Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A security document, comprising:

a printed document; and

one or more memory circuits configured to be read wirelessly and attached to or incorporated within the printed document,

wherein data in the memory circuit is protected from access by an ~~unauthorised~~ unauthorized reader,

wherein the memory circuit is physically isolated so as to inhibit physical tampering or is configured to indicate when physical tampering has occurred, and

wherein physical isolation of the memory circuit employs one or more tamper-evident strips.

2. (Original) A security document as claimed in claim 1, wherein the memory circuit is inductively powered.

3. (Original) A security document as claimed in claim 2, wherein the memory circuit receives and transmits data wirelessly at radio frequency.

4. (Cancelled)

5. (Currently amended) A security document as claimed in claim 1, wherein ~~an antenna of~~ the memory circuit includes an antenna that is configured for detection or resistance of physical tampering.

6. (Currently amended) A security document as claimed in claim 1, wherein the security document is configured to identify an ~~authorised~~ authorized bearer of the security document.

7. (Currently amended) A security document as claimed in claim 6, wherein the security document ~~is configured~~ includes means to allow access to a specified asset or assets by the ~~authorised~~ authorized bearer.

8. (Currently amended) A method of publishing a security document, comprising:

a. determining first information for printing in a printed document, and second information for writing to one or more memory circuits for attachment to or incorporation within the printed document;
b. protecting the second information from ~~unauthorised~~ unauthorized reading;
c. printing the first information in the printed document;
d. writing the second information to one or more memory circuits configured to be read wirelessly for attachment to or incorporation within the printed document; and
e. physically isolating the one or more memory circuits so as to inhibit physical tampering or configuring the one or more memory circuits to indicate when physical tampering has occurred.

9. (Currently amended) A method of reading a security document comprising a printed document and one or more memory circuits attached to or incorporated within the printed documents, comprising:

[[f.]] a. obtaining ~~authorisation~~ authorization information to read the security document;

[[g.]] b. reading first information printed in the printed document;

[[h.]] c. wirelessly powering at least one memory circuit and wirelessly reading protected second information stored in said memory circuit;

[[i.]] d. reading the second information by using the ~~authorisation~~ authorization information; and

[[j.]] e. using the second information with the first information to assess the security document.

10. (Original) A method as claimed in claim 9, further comprising comparing the second information to one or more characteristics of a bearer of the security document.

11. (Currently amended) A security document, comprising:

a printed document; and

one or more memory circuits configured to be read wirelessly attached to or incorporated within the printed document,

wherein data in the memory circuit is protected from access by an ~~unauthorised~~ unauthorized reader,

wherein the memory circuit is physically isolated so as to inhibit physical tampering or is configured to indicate when physical tampering has occurred, and

wherein both printed data and data in the memory circuit is configured to identify a bearer of the security document.

12. (Currently amended) A method of publishing a security document for a bearer, comprising:

[[k.]] a. determining first information concerning the bearer for printing in a printed document, and second information concerning the bearer for writing to one or more memory circuits for attachment to or incorporation within the printed document;

[[l.]] b. protecting the second information from ~~unauthorised~~ unauthorized reading;

[[m.]] c. printing the first information in the printed document;

[[n.]] d. writing the second information to one or more memory circuits configured to be read wirelessly for attachment to or incorporation within the printed document; and

[[o.]] e. physically isolating the one or more memory circuits in the printed document so as to inhibit physical tampering or to indicate when physical tampering has occurred.

13. (New) A security document as claimed in claim 1, wherein the one or more tamper-evident strips provide a visual indication as to whether or not the memory circuit has been physically tampered with.

14. (New) A security document as claimed in claim 1, wherein the one or more tamper-evident strips correspond to at least one cut on the printed document provided adjacent to the memory circuit.

15. (New) A security document as claimed in claim 1, wherein the printed document is a sheet of paper.

16. (New) A security document as claimed in claim 11, wherein the printed document is a sheet of paper.

17. (New) A method as claimed in claim 12, wherein the printed document is a sheet of paper.

18. (New) A security document as claimed in claim 1, wherein the one or more memory circuits are provided on an external surface of the printed document that is exposed to the environment.

19. (New) A security document as claimed in claim 11, wherein the one or more memory circuits are provided on an external surface of the printed document that is exposed to the environment.

20. (New) A method as claimed in claim 12, further comprising:

providing the one or more memory circuits on an external surface of the printed document that is exposed to the environment.

21. (New) A security document as claimed in claim 5, wherein the memory circuit includes means for detection a change in a physical property of the antenna, the change in the physical property being indicative of physical tampering of the antenna, wherein the memory circuit includes means for disabling reading of the memory circuit when the physical tampering of the antenna is detected.